IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

SABA MAHMOOD, individually and on behalf of similarly situated individuals, *Plaintiff*, v. BERBIX, INC., a Delaware corporation, *Defendant.*	No. 1:22-cv-02456 Hon. Sharon Johnson Coleman Magistrate Heather K. McShain

PLAINTIFF'S MEMORANDUM OF LAW
IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

Timothy P. Kingsbury
Andrew T. Heldut
MCGUIRE LAW, P.C.
55 W. Wacker Dr., 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
tkingsbury@mcgpc.com
aheldut@mcgpc.com

Attorneys for Plaintiff and the Putative Class

I. INTRODUCTION

Defendant Berbix, Inc. ("Defendant" or "Berbix") operates an Internet-based identity-verification platform. Unlike many other such platforms, Berbix's technology relies on automated biometric facial recognition technology to compare individuals' government IDs and pictures of their face in order to confirm that the government ID is valid. In 2020, Plaintiff Saba Mahmood ("Plaintiff") uploaded her government ID and a photograph of her face to Defendant's platform while she was in Illinois in order to rent a car from Audi SilverCar, one of Defendant's clients. She alleges that despite collecting and using her biometric data, Berbix failed to comply with the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), which regulates, among other things, private entities' collection and use of Illinois citizens' biometric data.

Defendant has moved to dismiss her claims under several theories, each of which should be rejected. Defendant's extraterritorial and dormant Commerce Clause challenges fail as they have been routinely rejected at the motion to dismiss stage by numerous courts, including this Court. Defendant offers no basis for a different result here. Defendant also attacks Plaintiff's 15(c) and 15(d) BIPA allegations as "speculative" and "conclusory," but the Complaint alleges enough facts to sustain both of these claims as well. Defendant also attacks Plaintiff's request for heightened damages, ignoring that the Complaint contains more than adequate support for the inference that Defendant's violations of BIPA were reckless or intentional.

For those reasons, and as discussed in further detail below, Defendant's Motion should be denied in its entirety.

II. FACTUAL ALLEGATIONS

Berbix is a developer and provider of online identity verification services, which include a biometric verification component, and integrates its service with its clients' websites and/or mobile

applications in order to verify its clients' users' identities. (Class Action Complaint, "Compl.," Dkt. 1-1, ¶ 20). Plaintiff registered with SilverCar by Audi, one of Berbix's clients, in Illinois in August 2020. (*Id*. ¶ 22). As part of the SilverCar's onboarding process through SilverCar's online application, Plaintiff was then required to use Berbix's photo ID verification portal, where she was required to upload her Illinois Driver's License as well as a separate "selfie" photograph. (*Id*. ¶ 23). Using facial recognition technology, Berbix scanned and compared the geometry of the face appearing on Plaintiff's Driver's License with the geometry of the face appearing in her "selfie" photograph in order to verify his identity. (*Id*. ¶ 24). Despite collecting Plaintiff's facial biometrics in Illinois, Berbix failed to obtain her informed consent to do so, failed to disclose to her the purpose of its biometric collection and the length of term for which her biometrics would be used, and failed to obtain her consent to disseminate his biometric data to others. (Id. ¶¶ 25-27). Accordingly, on April 4, 2022 Plaintiff filed this case against Berbix in Illinois state court under 740 ILCS 14/15(b), 740 ILCS 14/15(c), and 740 ILCS 14/15(d).

Notably, and as cited in Plaintiff's Complaint (¶ 21), Defendant's Privacy Policy[1] in effect when Plaintiff interacted with its identity-verification platform not only admits that Defendant collects and uses individuals facial biometric data, but that Defendant also collects various other forms of data, including individuals' geolocations and IP addresses. The Policy also states that Defendant discloses user data to third-party vendors, including the Google Cloud Platform, for data storage purposes.

III. LEGAL STANDARD

Where a defendant moves to dismiss a complaint under Federal Rule 12(b)(6), the motion does not test the merits of the plaintiff's claims; rather it "tests only the legal sufficiency of the

[1] A true and correct copy of Defendant's Privacy Policy is attached hereto as Exhibit A.

complaint." *Hanley v. Green Tree Serv., LLC*, 934 F. Supp. 2d 997, 980 (N.D. Ill. 2013) (citing *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990)). When considering a Rule 12(b)(6) motion, the court must construe the complaint "in the light most favorable to the nonmoving party, accept well-pleaded facts as true, and draw all inferences in [the plaintiff's] favor." *Kolbe & Kolbe Health & Welfare Benefit Plan v. Med. Coll. of Wis*., 657 F.3d 496, 502 (7th Cir. 2011).

A complaint will survive a Rule 12(b)(6) motion as long as it "contain[s] sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. A complaint "should not be dismissed for failure to state a claim unless it appears beyond doubt that the plaintiff is unable to prove any set of facts which would entitle the plaintiff to relief." *Supreme Auto Transport v. Arcelor Mittal*, 238 F. Supp. 3d 1032, 1036 (N.D. Ill. 2017) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 546 (2007)).

IV. ARGUMENT

A. Plaintiff Sufficiently Alleges That Defendant's BIPA Violations Occurred In Illinois.

Plaintiff alleges that she is an Illinois resident (Compl. ¶ 17) who – while in Illinois – accessed Defendant's client SilverCar's car rental app (*Id.* ¶ 22), which was integrated with Defendant's identity-verification platform (*Id.* ¶ 20). Thus, while using the SilverCar app in Illinois, Plaintiff had to upload her Illinois Driver's License and a "selfie" photograph to Defendant's platform (*Id.* ¶ 23), upon which Defendant extracted her facial biometrics (*Id.* ¶ 24). At the pleadings stage, when they must be construed in Plaintiff's favor, these allegations are sufficient to plausibly allege that Defendant's BIPA violations, including its failure to obtain Plaintiff's consent to biometric collection and dissemination, occurred primarily and substantially

in Illinois. Indeed, by alleging the exact steps Defendant took to collect Plaintiff's biometric data (scraped off her Illinois Driver's License) while she was in Illinois, Plaintiff shows a closer connection between Defendant's conduct and Illinois than the plaintiffs did in *In re Clearview AI, Inc., Consumer Priv. Litig.*, where this Court rejected the defendants motion to dismiss on extraterritorial grounds because the plaintiff alleged that they were "Illinois residents, the Clearview defendants failed to provide notice to the Illinois subclass members in Illinois, and defendants trespassed on the Illinois subclass members' private domains in Illinois. *In re Clearview AI, Inc., Consumer Priv. Litig.*, No. 21-cv-0135, 2022 WL 444135, at *4 (N.D. Ill. Feb. 14, 2022). And this Court is far from the only court in this Circuit to have held that purported extraterritoriality defenses should generally not be resolved at the pleadings stage, and instead should be left for the summary judgment stage following discovery. For instance, in *Rivera v. Google Inc.*, Judge Chang found that the plaintiffs' allegations that the defendant extracted biometric data from pictures uploaded by Illinois citizens using Illinois IP addresses while in Illinois were enough to "tip toward a holding that the alleged violations primarily happened in Illinois," permitting the plaintiffs to proceed with discovery. *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1102 (N.D. Ill. 2017); *see also Patel v. Facebook*, 932 F.3d 1264, 1276 (9th Cir. 2019) ("[I]t is reasonable to infer that the [Illinois] General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state."); *Vance v. Int'l Bus. Machines Corp.*, No. 20-cv-577, 2020 WL 5530134, at *3 (N.D. Ill. Sept. 15, 2020) (rejecting extraterritoriality defense at the pleadings stage because the defense requires a "highly fact-based analysis that is generally inappropriate for the motion to dismiss").

Defendant's argument to the contrary relies on an unreasonable misreading of the Complaint. Defendant pretends that all Plaintiff has alleged is that she is an Illinois resident, when

she clearly alleges she accessed the SilverCar application, and thus connected to Defendant's identify-verification platform, while she was in Illinois. (Compl. ¶¶ 23-24). Thus, the various cases Defendant cites where courts held that the plaintiff's residence cannot be the sole nexus between the unlawful conduct and Illinois are inapposite. Defendant's heavy reliance on an out of Circuit case, *McGoveran v. Amazon Web Servs.*, Inc., No. 20-1399-LPS, 2021 WL 4502089 (D. Del. Sept. 30, 2021), is also inapposite, because in that case the plaintiffs did not "allege any direct interaction with [the defendants] that might plausibly imputed to Illinois." 2021 WL 4502089 at *5. Here, in contrast, Plaintiff sufficiently alleges that she directly interacted with Defendant while ishe was in Illinois because she accessed SilverCar's application in Illinois, and in turn interacted with Defenadnt's facial recognition technology embedded in the SilverCar application.

For those reasons, the Court should reject Defendant's extraterritoriality argument at this stage of the litigation.

B. Applying BIPA To Defendant's Conduct Does Not Violate The Dormant Commerce Clause.

As an alternative to its extraterritoriality argument, but based on the same erroneous misreading of the Complaint, Defendant argues that applying BIPA to its collection of Illinois residents' biometric data would run afoul of the Dormant Commerce Clause. Because Plaintiff adequately alleges that Defendant's misconduct took place in Illinois, this argument should be rejected for the same reasons as Defendant's extraterritoriality argument. *In re Clearview AI, Inc.*, 2022 WL 444135 ("As with the Clearview defendants' related extraterritoriality arguments, whether BIPA controls commercial conduct that occurs wholly outside Illinois is a question best left for later in these proceedings after the parties have completed discovery")

Moreover, with respect to Defendant's argument that somehow Plaintiff's BIPA claims violate the Dormant Commerce Clause because "only three states have enacted biometric statutes"

and "any such construction would frustrate the policy decisions of the 49 states that have declined to regulate biometrics directly or at all,or have tasked only the state Attorney General with enforcement" (Mot. at 8), it is important to note that Defendant knows the geolocations (including GPS coordinates) of the individuals whose biometrics Defendant processes. (Ex. A at 2). Thus, it should be a relatively easy process for Defendant to comply with BIPA with respect to Illinois residents, but ignore BIPA's requirements when interacting with non-Illinois individuals. Put differently, applying BIPA to Defendant's conduct here would have no effect on its interactions with individuals from other states.

For these reasons, Defendant's arguments for dismissal on this basis should be rejected as well.

C. Plaintiff Adequately Alleges That Defendant Profits Directly From Biometrics In Violation Of Section 15(c).

Section 15(c) of BIPA provides that, "[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15/(c). Defendant violated this section because, as Plaintiff directly alleges, Defendant is paid by its clients for access to Defendant's facial recognition and matching platform on a per-biometric-transaction basis. (Compl. ¶ 43). In other words, biometrics are a necessary element of Defendant's profit model, supporting a claim that Defendant unlawfully generates profits resulted directly, and distinctly, from its collection and use of biometrics. *Flores v. Motorola Sols., Inc.*, No. 20-cv-01128, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021) (sustaining 15(c) claim because Section 15(c) prohibits incorporating biometrics as a "necessary element to [a] business model."). Indeed, this Court recently sustained similar Section 15(c) claims in *In re Clearview AI, Inc.,* where the plaintiffs alleged that Macy's acquired their biometric data from a third party and used the data for loss

prevention purposes, such that it was "reasonable to infer that plaintiffs' biometric information was necessary to Macy's loss prevention business model and that this biometric information generated profits by reducing the number of stolen goods." 2022 WL 252702, at *4. Here, similarly, the Court should sustain Plaintiff 's Section 15(c) claim because she plainly alleges that biometrics are necessary to Defendant's business model.

Plaintiff's claim is not, as Defendant wrongly suggests, only plead on "information and belief" (*see* Compl. ¶ 43), or a bald recitation of the statutory language. Rather, Plaintiff has satisfied her pleading burden under Fed. R. Civ. P. 8 by alleging precise facts (Defendant charges its clients on a per-biometric-verification basis) which put Defendant on notice of how Plaintiff alleges Defendant violated Section 15(c). Accordingly, Plaintiff states a claim under Section 15(c).

D. Plaintiff States A Claim Under Section 15(d).

Section 15(d) of BIPA prohibits the disclosure or dissemination of biometric identifiers or biometric information without a person's informed consent. See *Cothron v. White Castle Systems, Inc.*, 467 F. Supp. 3d 604, 613 (N.D. Ill. 2020) ("Section 15(d) requires entities to obtain a person's informed consent when disclosing or disseminating an individual's biometric data"). Defendant argues that Plaintiff's 15(d) claim fails as speculative and conclusory, suggesting that her claim is only plead on "information and belief," but conveniently ignores that the Berbix Privacy Policy cited in Paragraph 21 of Plaintiff's Complaint not only admits that "[Defendant] may share all personal information that we collect [including facial recognition data] with: Third-Party vendors and other service providers that perform services on our behalf" (Ex. A at 4), it also states that "Berbix uses Google Cloud Platform to store your data [including facial recognition data]." In other words, Plaintiff's Section 15(d) claim does not "parrot" the statutory language. Her claim is premised on Defendant's failure to obtain her consent to disclose her biometric data its third-party

vendors, including Google. "That is a textbook violation of § 15(d)." *Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 785 (N.D. Ill. 2020) (sustaining claim where plaintiffs alleged the defendant "disseminated [their] biometric data to other firms that hosted the information in their data centers" without their consent). Unlike in *Namuwonge v. Kronos, Inc.*, where the plaintiffs alleged that they "have no idea" whether biometrics were disseminated, 418 F. Supp. 3d 279, 285 (N.D. Ill. 2019), Plaintiff's claim here is supported by Defendant's own Policy which clearly states that it disseminates face geometry data to third parties. Defendant is free to dispute the accuracy of its own Policy during discovery, but at this stage, the Complaint alleges more than sufficient detail to state a Section 15(d) claim.

As a fallback, Defendant suggests that its dissemination of Plaintiff's biometrics to its third-party vendors somehow "complete[d] a financial transaction," such that its failure to obtain her consent is excused by 740 ILCS 14/15(d)(2). Defendant is simply wrong. Even assuming that any "purchase" qualifies as a "financial transaction" for purposes of 740 ILCS 14/15(d)(2) (which would render the exemption incredibly broad), and even assuming that Defendant's verification of Plaintiff's identity "completed" her transaction with SilverCar (a dubious theory considering that identity-verification was just one of many steps in SilverCar's rental process), Defendant does not, presumably because it cannot, explain any connection between Plaintiff's car rental and Defendant's decision to send Plaintiff's biometrics to third parties such as Google for data storage. The escape hatch Defendant seeks simply does not exist.

For those reasons, Plaintiff's Section 15(d) claim should be sustained.[2]

[2] In a footnote, Defendant discusses the statute of limitations applicable to Section 15(c) and (d) claims, but does not affirmatively argue that Plaintiff's 15(c) and (d) claims are time-barred. Presumably, Defendant does not do so because, as Defendant acknowledges, the accrual dates of those claims present factual questions unsuitable for resolution on a Motion to Dismiss. However, to the extent Defendant changes its position on Reply and substantively argues that any of Plaintiff's claims are untimely, Plaintiff reserves the right to seek leave to respond.

E. Plaintiff Sufficiently Alleges That Defendant's BIPA Violations Were Reckless Or Intentional.

Defendant also requests that the Court strike Plaintiff's request for heightened damages under 740 ILCS 14/20(2), arguing that the Complaint lacks sufficient facts to infer that Defendant's BIPA violations were reckless or intentional. Plaintiff acknowledges that this Court has previously stricken requests for such damages in the past, including where the plaintiff noted that the defendant had failed to comply with BIPA for years after its passage. *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 286 (N.D. Ill. 2019); *but see Rogers v. BNSF Ry. Co.*, No. 19-cv-3083, 2019 WL 5635180, at *5 (N.D. Ill. Oct. 31, 2019) ("[T]he BIPA took effect more than ten years ago, and if the allegations of his complaint are true—as the Court must assume at this stage—BNSF has made no effort to comply with its requirements. This is certainly enough, at the pleading stage, to make a claim of negligence or recklessness plausible"); *Wordlaw v. Enter. Leasing Co. of Chicago, LLC*, No. 20-cv-3200, 2020 WL 7490414, at *7 (N.D. Ill. Dec. 21, 2020) ("The complaint's allegation that in 2016, "defendants knew, or were reckless in not knowing" that the timekeeping system was subject to BIPA's requirements is plausible . . . Yet defendants made no effort to comply with BIPA. This is enough to allege a negligent, reckless, or intentional violation"); *Horn v. Method Prod., PBC*, No. 21 C 5621, 2022 WL 1090887, at *2 (N.D. Ill. Apr. 12, 2022) ("Rule 8 does not require a plaintiff to plead damages with particularity and instead only requires 'a demand for the relief sought'"); *Hedick v. The Kraft Heinz Co.*, No. 19-cv-1339, 2021 WL 3566602, at *3 (N.D. Ill. Aug. 11, 2021) (noting that the Seventh Circuit has cautioned against "piecemeal dismissals of *parts* of claims").

Here, Plaintiff's Complaint contains more detail than the complaint in *Namuwonge*. Defendant's Privacy Policy lends ample support for the inference that its failures to comply with BIPA's consent requirements were reckless or intentional. The Policy (dated March 11, 2019)

demonstrates that Defendant knew for at least a year before it collected and handled Plaintiff's biometric data in 2020 that its facial comparison practices would be subject to various privacy laws, including U.S. privacy laws such as BIPA. (*See* Ex. A at 4 ("If you are located in the European Union or other regions with laws governing data collection and use that may differ from U.S. law, please note that we may transfer information, including personal information, to a country and jurisdiction t*hat does not have the same data protection laws as your jurisdiction, including the U.S.* . . ") (emphasis added). The Policy also discusses privacy rights under European law (*Id.* at 5), and even seeks to explain Defendant's "legal basis for processing" various forms of user data (*Id.* at 1-3). In other words, Defendant was aware of its obligations to comply with the privacy laws of each of the jurisdictions in which it does business, such that its failures to obtain Plaintiff's consent for the collection and dissemination of her biometric data in compliance with BIPA are inexcusable.

In short, Plaintiff anticipates that discovery would reveal additional evidence that Defendant was aware of BIPA's consent requirements when it interacted with Plaintiff, but either recklessly or intentionally failed to provide her with the written disclosures mandated by Section 15(b) and failed to obtain Plaintiff's consent to the collection and dissemination of her biometric data. Thus, Defendant's request that the Court strike Plaintiff's request for heightened damages should be denied at this stage of the litigation.

V. CONCLUSION

For the foregoing reasons, Plaintiff Saba Mahmood respectfully requests that the Court deny Defendant's Motion to Dismiss in its entirety.

Dated: July 8, 2022

Respectfully submitted,

SABA MAHMOOD, individually and on behalf of similarly situated individuals

By: /s/ Timothy P. Kingsbury
One of Her Attorneys

Timothy P. Kingsbury
Andrew T. Heldut
MCGUIRE LAW, P.C.
55 W. Wacker Dr., 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
tkingsbury@mcgpc.com
aheldut@mcgpc.com

Attorneys for Plaintiff and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that, on July 8, 2022, I caused the foregoing *Plaintiff's Memorandum of Law in Opposition to Defendant's Motion to Dismiss* to be electronically filed with the Clerk of the Court using the CM/ECF system. A copy of said document will be electronically transmitted to all counsel of record.

/s/ Timothy P. Kingsbury